REMARKS

The Examiner is thanked for the careful review of the subject application. Claims 1, 3-7, 9-12, 14-17, and 19 are pending in the present application. Claims 2, 8, 13, and 18 have been canceled. Claims 1, 5, 10, and 15 have been amended to better define the claimed subject matter. The Applicant respectfully submits that the amendments do not include new matter. Therefore, after entry of the above amendments, claims 1, 3-7, 9-12, 14-17, and 19 will be pending in this application. The Applicant believes that the present application is now in condition for allowance, which prompt and favorable action is respectfully requested.

Rejection under 35 U.S.C. §102

The Office has maintained rejection of claims 1, 3-7, 9-12, 14-17, and 19 under 35 U.S.C. §102(e) as being anticipated by U.S. Publication No. 2003/0041167 to French et al. (hereinafter "French"). The Applicant respectfully traverses the Office's rejection as French fails to disclose each and every feature of amended independent claims 1, 5, 10, and 15, as described in more detail below.

As amended, among other features, independent claim 1 recites "wherein the protection system generates a digital signature for the geographic identifier associated with the application." In the same manner, independent claim 5 has been amended to recite, *inter alia*, "wherein a logic included in the geographic database generates a digital signature for the geographic indicator." Similarly, independent claims 10 and 15 have been amended to recite "wherein a digital signature is generated for the geographic indicator."

It is respectfully submitted that French fails to disclose each and every feature of amended independent claims 1, 5, 10, and 15. For instance, contrary to the subject application, there is no disclosure (or suggestion) in French that an application is associated with a

geographic indicator or identifier or that a digital signature is generated for the geographic identifier or indicator.

Citing to paragraph 16 of French in the Final Office Action and the Advisory Action, the Office has rejected the Applicant's interpretation. Specifically, the Office has asserted that the network resources disclosed in French correspond to the application, as recited in independent claims 1, 5, 10, and 15. The Office has further interpreted that the geographic location identifiers of French are the same as the geographic indicator of the subject claims because the geographic location identifiers of French are associated with the network resources (components interpreted by the Office to be the application of the claims). The Applicant respectfully traverses the Office's assertion, as contrary to the Office's assertion, the geographic location identifier of French is not the same as the geographic identifier of the subject application. Support for the Applicant's interpretation is provided in paragraph 316 of French, which in pertinent parts provides:

> . . . *A geographic location identifier is automatically generated for an endpoint based on the endpoint's MAC address and its relation to a router within its network, thereby uniquely identifying the endpoint using the endpoint's hardware MAC address in conjunction with its geographic location.* Network-related actions can be performed on resources with common geographic locations. Security attributes can automatically be associated with the endpoint based on the endpoint's current geographic location, and administrative GUI notification events occur only in response to *potential security breaches and not merely in response to a change in geographic location of an endpoint.* The present invention effectively introduces the ability to implement security-related commands such that actions can be authorized with respect to geographic locations. [Emphasis added.]

As evidenced by the reproduced excerpt, the geographic location identifier in French is disclosed to be related to the endpoint's MAC address and the endpoint's relation to a router within its network, and not related to any information associated with the resource, itself.

Additionally, even if the geographic location identifier of French were the same as the geographic identifier of the subject application (a proposition with which the Applicant disagrees), French does not disclose (or suggest) that a digital signature is generated. Even if a digital signature is generated in French (a proposition with which the Applicant disagrees), there is no disclosure (or suggestion) in French that the digital signature is generated for the geographic location identifier.

The Applicant respectfully traverses the Office's assertion that French discloses generating a digital signature for the geographic identifier. In support of the Office's assertion, the Office has cited to paragraphs 91, 94, 97, 166, 217, and 259 of French. It is respectfully asserted that contrary to the Office's contention, none of the cited paragraphs disclose (or suggest) that a digital signature is generated for the geographic location identifier in French. For instance, paragraph 91 provides:

> Queuing the action object on the gateway results in a controlled process for the sending and receiving of data from the IP devices. As a general rule, the queued action objects are executed in the order that they arrive at the gateway. The action object may create child action objects if the collection of endpoints contains more than a single ORB ID or gateway ID. The parent action object is responsible for coordinating the completion status of any of its children. The creation of child action objects is transparent to the calling application. A gateway processes incoming action objects, assigns a priority, and performs additional security challenges to prevent rogue action object attacks. The action object is delivered to the gateway that must convert the information in the action object to a form suitable for the agent. The gateway manages multiple concurrent action objects targeted at one or more agents, returning the results of the operation to the calling application as appropriate.

It is submitted that contrary to the Office's assertion, nothing in the cited paragraph is directed at generating digital signatures, and more importantly, at generating a digital signature for the geographic location identifier.

In the same manner, nothing in paragraph 94 of French discloses (or suggests) generating a digital signature for the geographic location identifier. Specifically, paragraph 94 provides:

> The AOIP class should include the following: a constructor to initialize itself; an interface to the NELS; a mechanism by which the action object can use the ORB to transport itself to the selected gateway; *a security check verification of access rights to endpoints*; a container for either data or commands to be executed at the gateway; a mechanism by which to pass commands or classes to the appropriate gateway or endpoint for completion; and public methods to facilitate the communication between objects. [Emphasis added.]

Essentially, paragraph 94 indicates that the AOIP class includes a security check verification of access rights to endpoints. Such reference to security check, on the other hand, does not disclose (or suggest) generating a digital signature for the geographic location identifier.

Similarly, paragraph 97 provides:

> The NELS service finds a route to communicate between the application and the appropriate endpoint. The NELS service converts input to protocol, network address, and gateway location for use by action objects. The NELS service is a thin service that supplies information discovered by the IPOP service. The primary roles of the NELS service are as follows: support the requests of applications for routes; maintain the gateway and endpoint caches that keep the route information; *ensure the security of the requests*; and perform the requests as efficiently as possible to enhance performance. [Emphasis added.]

Yet again, ensuring the security of requests does not disclose (or suggest) generating a digital signature for the geographic location identifier. In the same manner, nothing in paragraph 166 discloses (or suggests) a digital signature. Specifically, paragraph 166 provides:

> With reference now to FIG. 6, a block diagram shows a set of components that may be used to implement scope-based security access in the present invention. *Login security subsystem 602 provides a typical authentication service, which may be used to verify the identity of users during a login process.* All-user database 604 provides information about all users in the DKS system, and active

> user database 606 contains information about users that are currently logged into the DKS system. [Emphasis added.]

As evidenced by the cited excerpt, paragraph 166 is directed at an authenticating service used to verify the identity of the user. It is respectfully submitted that verifying the identity of the user is not disclosed (or suggested) to be related to the geographic location identifier of French. Furthermore, nothing in the cited paragraph discloses any information as to generating a digital signature for the geographic location identifier.

Similarly, paragraph 217 of French fails to disclose (or suggest) generating a digital signature for the geographic location identifier. Rather, paragraph 217 provides:

> With reference now to FIG. 11A, a block diagram shows a set of components that may be used to implement multi-customer management across multiple networks in which duplicate addresses may be present. FIG. 11A depicts components that are similar to components introduced in other figures above. *User security subsystem 1106 provides a user authentication and authorization service, which may be used to verify the identity of users, such as administrators, during a login process and during administrative operations.* IP drivers 1108 detect IP objects within an IP network. Gateway/NEL service 1110 provides action object processing within gateways. A persistent repository, such as IPOP database 1112, is updated to contain information about the discovered and monitored IP objects. Other ORB or core services 1114 may also access IPOP database 1112. [Emphasis added.]

It is respectfully asserted that providing a user authentication and authorization service does not disclose (or suggest) generating a digital signature for the geographic location identifier.

Lastly, paragraph 259 of French provides:

> As noted previously, given a scenario in which a multi-customer service provider is operating an integrated network management system for multiple customers, it is likely that many individuals will be assigned to manage different regions and different groups of devices. In addition, these individuals may have different duties within geographically dispersed portions of the network, such as various customer sites, and these individuals may belong to many different organizational groups, either within the service provider's organization or within one of the customer's organization. In a highly distributed system comprising on the order of a million devices, *the task of authenticating and authorizing the*

> *administrative actions of many individuals per customer, per region, per device, etc., becomes quite complex.* [Emphasis added.]

Once again, it is respectfully submitted that contrary to the Office's assertion, authorizing and authenticating administrative actions does not disclose or suggest generating a digital signature for the geographic location identifier associated with an application.

Still further, as amended, independent claims 1 and 5 respectively recite "sending an authorization code to allow an execution of the application if the device is within the predetermined operating region," and "if the device is within the predetermined operating region, an authorization code is generated so as to allow the application to operate." In the same manner, independent claims 10 and 15 respectively recite "means for sending an authorization code to allow an execution of the application if the device is within the predetermined operating region," and "instructions for sending an authorization code to allow an execution of the application if the device is within the predetermined operating region." It is respectfully submitted that in contrast to claims 1, 5, 10, and 15, French does not disclose or suggests sending an authorization code to allow the network resources to execute or operate.

The Applicant further incorporates by reference the Applicant's arguments provided earlier in the Amendment filed on April 28, 2006 and the Request for Reconsideration filed on August 27, 2006, in their entirety.

Based on any of the aforementioned reasons, the Applicant respectfully requests that the Office withdraw the rejection of claims 1, 3-7, 9-12, 14-17, and 19 under 35 U.S.C. § 102.

CONCLUSION

In light of the amendments contained herein, Applicants submit that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated October 11, 2006

By: /Fariba Yadegar-Bandari/
Fariba Yadegar-Bandari
Reg. No. 53,805
(858) 651-0397

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-5787
Facsimile: (858) 658-2502